FFIEC IS EXAMINATION POLICY ISSUANCES

CHAPTER 25

(FILE NAME ON DISK # 2 = S3C25.WPD)

TABLE OF CONTENTS

		OCC-BC-271 (5-25-93) FDIC-FIL-30-93 (4-29-93)	OTS-TB 59 (5-19-93)
SP-10	**12/93**	**Interagency Document on Control and Security Risks in Electronic Imaging Systems** *Cross references:* FRB-SR-94-2 (1-13-94) FDIC-FIL-13-94 (2-25-94)	OCC-94-8 (1-27-94)
SP-11	**01/95**	**Enhanced Supervision Program (ESP) for Multidistrict Data Processing Servicers (MDPS)** *Cross references:* None	

Federal Financial Institutions Examination Council

SP-1
September 1991 Revised

Subject: Interagency EDP Examination, Scheduling And Distribution Policy

Purpose

This policy provides for joint examinations of data centers providing services to insured institutions supervised by more than one federal regulatory agency. It is expected to eliminate the need for separate examinations of data processors by more than one federal financial institution regulator and to result in more efficient use of examiner resources. This policy supersedes the previously issued interagency EDP examination policy, including the Multiregional Data Processing Servicers policy.

I. Examination Responsibility

Examination responsibility is determined based on the class/type of servicer as well as the class/type of insured financial institution(s) being serviced.

A. *Insured Institutions*

Data centers operated by an insured financial institution or its subsidiary will be examined by the federal regulatory agency responsible for the institution.

B. *Financial Institution Holding Companies*

Data centers operated by a holding company or its affiliate which service only one class of insured financial institution will be examined by the federal regulatory agency responsible for that class of institution.

Data centers operated by a holding company or its affiliate which service more than one class of insured financial institution will be examined jointly, or on a rotated basis, as agreed to by the federal regulatory agencies responsible for that class of institution.

Data centers operated by a holding company which controls only one insured financial institution, or its affiliate, will be examined by the federal regulatory agency responsible for the institution.

C. *Independent Data Centers*

Responsibility for the examination of independent data centers will be based on the class of insured financial institution being serviced. If more than one class of insured institution is serviced, the examination will be conducted jointly, or on a rotated basis, as

agreed to by the federal regulatory agencies responsible for that class of institution.

D. *Financial Institution Service Corporation*

Responsibility for the examination of service corporations will be based on the class of insured financial institution being serviced.

E. *Multiregional Data Processing Servicers (MDPS)*

MDPS examinations are to be conducted on a joint basis by the federal agencies having responsibility for the class of institution serviced. MDPS examinations will be administered by the FFIEC EDP Subcommittee of the Task Force on Supervision in Washington, D.C. The EDP subcommittee will determine the data centers subject to examination under the MDPS program. Generally, an organization will be considered for examination under the MDPS program provided: the organization processes major applications for a large number of insured financial institutions, thereby posing a high degree of systemic risk; or the organization processes work from a number of data centers located in diverse geographic regions.

No federal regulatory agency is precluded from conducting an independent examination of any data center that is providing data processing services to an insured financial institution for which the agency is responsible or where an agency has regulatory responsibility for holding company data centers.

II. Scheduling

Scheduling of joint/rotated EDP examinations and issuance of the EDP Report of Examination will be handled at the regional/district level. However, the examination of data centers under the MDPS program will be administered at the national level. A list of regions and contact personnel will be forwarded under separate cover and will be revised as appropriate.

A. *Joint and Rotated Examinations*

Regional/district representatives should meet annually (as early in the scheduling cycle as possible, but not later than December 1) to arrange for upcoming examinations and ensure that all data centers are examined in accordance with existing agency guidelines. As regional/district boundaries vary, it may be necessary for an agency to send representatives from more than one regional/district office to attend the scheduling meeting. Conversely, a representative may be required to attend more than one meeting. State agencies interested in participating in joint examinations may be invited to these meetings as deemed appropriate.

The meeting should identify all data centers, except for MDPS. Examinations of these data centers are to be conducted jointly and examination schedules agreed upon by participating agencies. If an agency cannot complete its schedule as agreed, it shall promptly notify the appropriate agencies so that alternative arrangements can be made.

When joint examinations cannot be scheduled, one agency will be designated to perform the examination on behalf of all concerned agencies. In these situations, examination responsibilities will be rotated for two-year periods. However, when the data center's overall condition is determined to be less than satisfactory, subsequent examinations should be conducted on a joint basis until the data center's overall condition is satisfactory as defined in the EDP Examination Handbook policy statement SP-2:

Uniform Interagency Rating System For Data Processing Operations.

The regional examination schedule should establish: the data centers to be examined; the date, time and agency responsible for any rotated or joint examinations; and the agency responsible for authoring and processing the examination report.

B. *Multiregional Data Processing Servicers*

Scheduling of MDPS examinations will be the responsibility of the FFIEC EDP Subcommittee of the Task Force on Supervision. By September 30 of each year, the EDP Subcommittee will prepare and publish an annual schedule for MDPS examinations designating the data center, the date of examination and the lead agency. This schedule will be distributed by the EDP Subcommittee agency representatives to their regional/district offices as soon as practical. An agency will be in charge of no more than two consecutive MDPS examinations.

Institutions with a composite rating of 1 or 2 will be subject to a full examination on a 24 month examination cycle, 3 rated institutions should be examined at an 18 month cycle and those institutions rated 4 or 5 at a 12 month cycle. The ongoing condition of MDPS should be monitored between examinations through periodic visitations and progress reports, as appropriate.

The lead agency is responsible for conducting a pre-examination review to determine: the scope of the examination, resource requirements, schedule of events and procedures to be followed during the course of the examination. At minimum this pre-examination report should provide details on the organization's: corporate history, corporate and organizational structure, scope of the upcoming examination, data centers included in the examination and examiner requirements. The pre-examination report should be forwarded to the Washington, D.C. office of the lead agency at least 60 days prior to the commencement of the MDPS examination.

Examinations of individual data centers or processing sites may commence prior to the start of the headquarters examination if more than one facility is involved. However, these time frames must be approved by the lead agency.

III. Report Preparation

A. *Joint Examinations*

Responsibilities will be divided among the EDP examiners assigned to the examination. When preparing joint examination reports, the participating agencies are required to reach agreement on the report comments. In rare instances when agreement cannot be reached at the regional level, the differences should be appealed to the Washington office of the participating agencies for final resolution.

The processing of the final Report of Examination (FFIEC 007) is the responsibility of the authoring agency. All changes made to the joint report in the course of its processing should be approved by the regional staffs of the agencies participating in the examination.

B. *MDPS Examinations*

Only one consolidated Report of Examination will be prepared by the lead agency. The

objective is to give the overall view of the organization, not each individual data center comprising the Multiregional Data Processing Servicer. However, the relative strength of each facility should be evaluated. In some instances it may be necessary to issue a specific data center report, although such action would be taken at the discretion of the EIC and the lead agency's Washington office.

IV. Report Distribution Policies and Procedures

A. *Joint Examinations*

The lead agency is responsible for providing each affected federal and state banking agency with a copy of the completed report, including the Administrative Section. (A complete list of all serviced financial institutions, by charter, should be included in this section as well.) Each agency is responsible for reproducing the report

comments and distributing them to serviced institutions in accordance with the provisions below. A transmittal letter will be used to advise each recipient that the comments are for their internal use only, are not to be construed to satisfy audit requirements and remain the confidential property of the lead agency. A written receipt will be obtained from each recipient.

In all instances, examination reports should be distributed to the board of directors of the examined data center. Where the data center is a subsidiary of a holding company, the report should be forwarded to the board of directors of the data center, where applicable, or otherwise senior management of the data center and to the board of directors of the holding company. In the case of a service corporation, a copy should be forwarded to the corporation's board of directors as well as to the board of directors of each financial institution owning stock in the corporation.

Independent Service Bureau reports should be directed to the board of directors or senior management of the servicer. If the independent service bureau is a branch of a multi-branch servicing organization, an additional copy should be forwarded to the board of directors at the corporate headquarters.

Distribution of examination reports to serviced institutions for joint examinations will be at the discretion of the federal regulatory agency responsible for regulating the institution serviced, except for data centers rated composite 4 or 5, which must be distributed to all insured serviced institutions. Where an examination report is to be distributed by a participating agency, the lead agency must be so notified prior to transmitting the examination report. When an examination report is requested by a serviced financial institution, only the examiner's conclusions, recommendations and comments are to be transmitted to the serviced institutions. Matters of a proprietary or competitive nature relating to the servicer will be excluded from the report comments prepared for distribution to serviced institutions, but will be contained in the report provided to the servicer and the other federal agencies. In cases where the servicer fails to respond to corrective action requests, it may be necessary to report the uncorrected deficiencies to the serviced institutions. In these situations, the regulatory agencies of all serviced institutions must be in agreement regarding the need for this course of action and must meet with the servicer to convey this intent.

The FFIEC interagency procedures do not affect existing distribution agreements with state agencies. However, no state agency shall distribute examination reports to any serviced institution without the express consent of the lead agency. Only the agency

conducting the examination will provide nonparticipating state authorities copies of the report. In the case of joint examinations, participation by state agencies and report distribution to those state agencies will be decided on an individual basis at the district/regional level by the participating federal agencies.

B. *MDPS Examinations*

The consolidated report of examination should be sent to the Washington office of the lead agency and to the board of directors of the data servicer. The lead agency's Washington office is to provide a copy of the report to the other FFIEC EDP Subcommittee members for distribution to the respective agency regional/district offices. The agency in charge is responsible for sending a copy of the report to the appropriate state supervisory agencies. Excluding the provisions noted above, distribution of MDPS reports should otherwise be in accordance with the provisions governing the distribution of joint interagency examinations.

Federal Financial Institutions Examination Council

SP-2
October 1978

Subject: Uniform Interagency Rating System For Data Processing Operations

The rating system for data processing operations is similar to the "Uniform Interagency Bank Rating System," which is based upon an evaluation of the overall performance of a bank. The EDP rating system is based upon an evaluation of four critical functions of a data processing operation: audit, management, systems development and programming, and computer operations. Each data center will be assigned a summary or composite rating based upon the separate performance ratings assigned these four functions.

Each performance rating and the composite rating are based on a scale of 1 through 5, with 1 representing the highest and 5 the lowest rating. Each function must be evaluated in order to determine its performance rating. To arrive at composite rating, due consideration must be given to the interrelationships and relative importance of the four functions. Occasionally there will be factors that are not reflected in any specific performance rating but are important to the data center's overall condition and should be reflected in the composite rating.

A general description of each performance rating is as follows:

Rating No. 1 – Strong performance.

Performance that is significantly higher than average.

Rating No. 2 – Satisfactory performance.

Performance that is average or slightly above and which adequately provides for the safe and sound operation of the date center.

Rating No. 3 – Fair performance.

Performance that is flawed to some degree and is considered to be of below average quality.

Rating No. 4 – Unsatisfactory performance.

Performance that is significantly below average and, if left unchecked, might evolve into weaknesses or conditions which could threaten the integrity of the records processed and the viability of the institution or data center.

Rating No. 5 – Hazardous performance

Performance that is critically deficient and in need of immediate remedial attention. Such performance threatens the integrity of the records being processed and the viability of the institution or date center.

A general description of each composite rating is as follows:

Composite 1 Data centers in this group are sound in almost every respect. If deficiencies are noted, they are of a minor nature and can be handled in a routine manner with out further supervisory involvement.

Composite 2 Data centers in this group are also fundamentally sound but may reflect modest weaknesses. Deficiencies are generally corrected in the normal course of business. Therefore, the need for supervisory response is usually limited.

Composite 3 Data centers in this group are experiencing a combination of adverse factors which require prompt corrective action. Problems are well defined and require more than ordinary supervisory concern and monitoring. The overall strength of management and supporting staff and the financial capacity of the data center are such as to make operation failure only a remote possibility.

Composite 4 Data centers in this group are operating under unacceptable conditions which could impair future viability. A high potential for operational and/or financial failure is present. Although a high potential for failure is present, weaknesses are not so severe as to threaten the immediate failure of the data center. Immediate affirmative action and supervision by the regulator are necessary.

Composite 5 Data centers in this group exhibit a combination of weaknesses and adverse trends which are pronounced to a point where the ultimate continuation of the operation is in serious question. Immediate affirmative action and continuous supervision, as required by the regulator, are necessary.

The four functional areas which are rated and the areas of consideration under each one are:

AUDIT

Audit is rated (1 through 5) with respect to:

A. Organization
- Independence
- Board of directors' support
- Resources allocated
- Management and staff succession

B. Staff Qualifications Training

C. Quality of Audits Scope
Frequency
Standards and procedures
- adequacy
- compliance

Follow up and correction of exceptions
Working papers and documentation
- completeness
- security

Audit software
- use
- effectiveness
- documentation

Audit reports

MANAGEMENT

Management is rated (1 through 5) with respect to:

A. Organization
Resources allocated
Leadership
Administrative abilities
Qualifications
Delegation of responsibilities
Support
Management succession

B. Correction of Deficiencies

C. Laws and Regulations
Awareness
Compliance
Contracts

D. Planning
Risk analysis
User involvement
Senior management involvement
Budget

E. Standards and Procedures
Development
Enforcement

F. Internal Controls
Development
Enforcement

G. Physical Security
Development
Enforcement

H. Financial Condition

SYSTEMS DEVELOPMENT AND PROGRAMMING

Systems and programming is rated (1 through 5) with respect to:

A. Organization
Separation of duties
Resources allocated
Management and staff succession

B. Staff
Qualifications
Training

C. Standards and Procedures
Adequacy
Compliance
User liaison

D. Documentation
Completeness
Organization
Storage and security

E. Internal Controls
Modification and change procedures
authorization
– documentation
– implementation
Program library maintenance
Systems development

F. Physical Security
Documentation
Software
On-line systems

Management and staffing
succession

B. Staff
Qualifications
Training

C. Standards and Procedures
Adequacy
Compliance
User liaison

D. Operations
Data entry control
Processing controls
Output distribution controls
Physical security
Emergency plans
User communication

COMPUTER OPERATIONS

Computer operation is rated (1 through 5)
with respect to:

A. Organization
Separation of duties
Resources allocated

Federal Financial Institutions Examination Council

SP-3
January 1988

Subject: Joint Interagency Issuance on End-User Computing Risks

To: Chief Executive Officers of all Federally Supervised Financial Institutions, Senior Management of each FFIEC Agency, and all Examining Personnel

Purpose:

The purpose of this issuance is to alert management of each financial institution of the risks associated with end-user computing operations and to encourage the implementation of sound control policies over such activities.

Background:

In recent years, microcomputers, or "personal computers", have become more prominent in the business environment. They are now being used, not only as word processors and access devices to other computers, but also as powerful stand-alone computers. As such, information processing has evolved well beyond the traditional central environment to distributed or decentralized operations. This trend has offered substantial benefits in productivity, customization, and information access. However, it also has meant that those control procedures, previously limited to the central operations, must be reapplied and extended to the "end-user" level.

Concerns:

Technology, using microcomputers as end-user computing devices, has taken data processing out of the centralized control environment and introduced the computer related risks in new areas of the banks. However, the implementation of these new information delivery and processing networks has out paced the implementation of controls. Basic controls and supervision of these computer activities often have not been introduced, or expected, at the end-user level. The technological advantages, expediency, and cost benefits of end-user computing has been the primary focus. Recognition of the increased exposures and the demands for expanded information processing controls has lagged. These concerns for data protection and controlled operations within the end-user environments must be addressed to minimize risks from:

- incorrect management decisions,
- improper disclosure of information,
- fraud,
- financial loss,
- competitive disadvantage, and

- legal or regulatory problems.

End-user computing is recognized as a productive and appropriate operational activity. However control policies for data security and computer operations, consistent with those for centralized information processing functions, need to address the additional risks represented in the end-user computing operations.

Bank management is encouraged to evaluate the associated risks with its end-user computing networks and other forms of distributed computer operations. Control practices and responsibilities to manage these activities should be incorporated into an overall corporate information security policy. Such a policy should address areas such as:

- management controls,
- data security,
- documentation,
- data/file storage and backup,
- systems and data integrity,
- contingency plans,
- audit responsibility, and
- training.

Responsibilities for the acquisition, implementation and support of such networks should be clearly established.

The appendix to this issuance provides more detail regarding the risks and suggested controls for end-user computing and other computer related activities. Additional control recommendations can be referenced in the FFIEC EDP Examination Handbook.

Policy:

It is the responsibility of the Board of Directors to ensure that appropriate corporate policies, which identify management responsibilities and control practices for all areas of information processing activities, has been established. The existence of such a "corporate information security policy," the adequacy of its standards, and the management supervision of such activities will be evaluated by the examiners during the regular supervisory reviews of the institution.

SP-3 - APPENDIX

Risks And Controls In End-User Computing

Microcomputers, in the end-user computing operations, are being used basically for three purposes:

1) as word processors,

2) as communications terminals with other computers (to transmit or receive information in their databases), and

3) as stand-alone computer processors.

These three functions require different control objectives, based on the risks associated with the activity. Each function requires certain operational type controls such as physical security, logical security, and file backup. However, the more pronounced risks involve those operations using microcomputers as stand-alone processors.

While word processing and terminal communications also require strong controls, programming support for the operating software and applications systems generally remain centralized or is a vendor responsibility. In end-user computing, the user is often engaged in program development, in addition to information processing. This may involve the creation of programmed software from an original design or building customized routines from specialized vendor software. Regardless, the control techniques for the programming, its testing, and its documentation are necessary to ensure the integrity of the software and the production of accurate data.

In addition to the programming activity, the end-user environment supports computer processing, which may be totally separate from centralized controls. Information may be downloaded from the main databases and reprocessed by the end-user. Data may also be originated for processing in this structure. Regardless of the source, the resulting information is relied upon by management for decisions impacting corporate strategies and customer relationships. The integrity of the data becomes no less important than had the data been produced through more sophisticated computer processes. Likewise, the need for control at the micro level remains equally important.

Impacts

The failure to properly implement a uniform set of controls on the end-users of microcomputers, consistent with those controls required in a mainframe data center, can create two broad categories of risks:

1) the corruption or loss of data and/or program software, and

2) impediments to the efficient operation and management of the bank.

The quality of data is paramount to the successful management of any institution. Should the data, or the systems which produce that data, be corrupted, whether intentionally or unintentionally, financial loss is highly probable. Data corruption could result from three basic causes: error, fraud, or system malfunction.

In addition to accuracy, management requires the timely availability of data. Inefficiencies,

caused by poor operational controls, can further impede the production of information and result in financial loss. Regardless of the source, poor quality information and operations can adversely impact the bank in a number of ways:

- *Management Error* – Inaccurate or incomplete data can adversely influence bank management decisions. Delays in information availability can also adversely impact corporate strategies.
- *Inadvertent Disclosure* – Human error, fraud, or system malfunction may result in proprietary bank data, customer data, or program software being disclosed to unauthorized persons.
- *Competitive Disadvantage* – Problems in the production of accurate and timely information can place the bank at a competitive disadvantage. Delivery of services, customer confidence, and management decisions could be impaired.
- *Legal Problems* – Errors in the production of data or wrongful disclosure of data may result in legal actions against the bank by its customers, consumer groups, competitors, and regulators.
- *Regulatory Problem* – Failure to produce timely and accurate data can cause the bank to be in violation of regulatory requirements, subjecting the bank to regulatory penalties.
- *Monetary losses* to the bank can arise from deliberate manipulation of the data (fraud), missing or erroneous data (leading to costly incorrect decisions), or various inefficiencies in the operation of the system.

Controls

There are basic controls which should be present in any level of computer operations. These controls should already be present at the centralized data center. The evolution of microcomputer-based systems has not eliminated the need for these basic controls, but has shifted the focus of control to the end-user level.

Some of these basic control standards that need to be implemented in microcomputer-based systems are:

Policies and Procedures

Control requirements for microcomputer use need to be addressed by management in its internal policies and procedures. Policies and procedures should be in writing and should define what steps are to be taken to protect the bank's microcomputer systems. Management should also designate responsibility within the bank to monitor microcomputer system acquisition and use. The purpose of this function should be to help prevent redundant uses of microcomputer systems and to ensure that there is the required degree of compatibility among hardware and software systems in use throughout the bank.

Program Development and Testing

Before a new system is developed or purchased, the user should have a clear understanding of the specific needs being addressed by the proposed new system. Alternatives should be reviewed by the user and analyst to ensure that the best solution is selected. Development should be done with the aim of producing a system that is easily modified and maintained by someone other than the original developer. Finally, the completed system should be subject to rigorous testing to provide

assurance that the results produced are valid and reliable.

Program Changes

Just as with larger systems, microcomputer systems must be adapted to meet changing requirements and circumstances. Modified programs should be subject to many of the same controls as newly-developed systems. Most important among these is the requirement that there be thorough testing of the modified system. In addition, accurate records should be maintained describing the change, the reasons for the change, and the person responsible for making the change.

Documentation

Documentation is a potential problem in microcomputer-based systems. There is a tendency for these systems to be highly personalized, with one person fully responsible for the development, testing, implementation, and operation of a set of programs. The successful use of a microcomputer-based system and the production of specialized data may depend on the continued presence of this one person. An adequate level of documentation helps to prevent an over reliance on the knowledge of this one person. This is particularly needed should revisions to programs be required. Documentation standards should define acceptable levels of program, operating, and user documentation. In addition, there should be an enforcement mechanism to guarantee compliance with standards.

Data Editing

The development or purchase of microcomputer systems should be done with adequate attention given to the need for data editing routines. These routines are important to help ensure that data entering the system is error-free and not likely to result in erroneous output. This control is important whether the data is being manually entered into the microcomputer or electronically transferred or "downloaded" from another system. In the case of data being "uploaded" to a mainframe, additional controls may be required at that level to guarantee the integrity of the data being transferred.

Input/Output Controls

Microcomputer systems that are used for the processing of information with a direct monetary impact on the bank or its customers may require that additional data controls be established. At a minimum, these controls may include the requirement that there be a segregation of duties between the input of information and the review of that information in processed form. This control may be extended to require that a formal reconcilement be done by the reviewer of the processed information. In more sensitive situations with a significant dollar impact, there may be a requirement that certain functions be performed under dual control. The need for these types of input and output controls should be established during the early stages of program development. These special requirements need to be described in detail in the program documentation package.

Physical Access Restrictions

The location of microcomputer systems outside of a physically-secure data center can permit unauthorized access to programs and data files used on these systems. The use of physical access restrictions complements the logical access restrictions discussed below. Basic steps would include the secure storage of diskettes or other magnetic media containing the programs and data for a particular system. In addition, since documentation on what a system does and how it is being used can provide important information that can be used to compromise system security,

this information should also be secured. Finally, there should be adequate restrictions over physical access to the hardware itself, so that it is protected from unauthorized use, vandalism, and theft.

Logical Access Restrictions

Just as in larger application systems, the need exists to identify those individuals who will be permitted access to the microcomputer system's capabilities. In addition, there may be the need to differentiate between functions allowed for certain individuals, ranging from an inquiry capability for many persons to an override and correction capability for a few supervisory personnel. Normally, these restrictions will be in the form of password controls. Standard password-related control procedures, such as frequent changes and reporting of exception conditions need to be established to provide for effective access restrictions.

Backup and Contingency Planning

For each operational system, adequate plans should be made and precautions taken to ensure that users can adequately recover from damage to the hardware, software, and data. For some systems, an inability to process during recovery may mean that work can be held for later processing. For other systems, a manual backup may be appropriate. For some time critical, highly automated systems, arrangements may have to be made for data reconstruction or for processing on other hardware. At a minimum, for all systems, there should be secure and remote backup storage of data files and programs. Beyond this, the backup and contingency requirements for individual systems may differ and need to be addressed separately.

Audit

The audit area should serve as an independent control reviewing microcomputer use throughout the bank. Audit involvement in microcomputer systems may begin at a general level with a review for compliance with the internal policies and procedures discussed above and may extend to detailed testing in particular areas such as the use of logical access controls. Audit procedures and workprograms should be expanded to provide for adequate coverage of microcomputer systems. Responsibility for microcomputer auditing should be clearly assigned and plans for microcomputer audits should be built into the audit schedule.

It should be recognized that this list of controls is not all inclusive of methods to manage risk. Each computer operation. Whether centralized or end-user, possesses different characteristics and possibly some specialized risks. Control practices must be sufficient to minimize such risks. These recommended control features are considered fundamental to sound information processing.

Federal Financial Institutions Examination Council

S P - 4

November 1988

Subject: Supervisory Policy On Large Scale Integrated Financial Software Systems (LSIS)

To: Chief Executive Officers of all Federally Supervised Financial Institutions, Senior Management of each FFIEC Agency,and all Examining Personnel

Financial institutions have experienced significant problems in attempts to introduce LSIS systems.

- After 2-1/2 years in development, one financial institution abandoned $20 million large scale integrated system!
- After 5 years in development, a major software vendor abandoned $100 million integrated system once described as the perfect software system for regional banks!

Purpose

Financial institution executives and directors should be aware of and concerned about the potential problems with LSIS. The purpose of this paper is to alert financial institutions to the risks associated with these systems and to identify management's responsibilities when entering into an LSIS project.

Background

"An integrated software system is one in which programs for different applications – loans, deposits, retail, and wholesale – that normally are designed and operated as stand alone programs are built from the start as related parts of a whole. They share a common language, operating system, and other technical details so that they can be made to `talk' to each other with relative ease. More importantly, they function as one unit so that the sum of the parts is greater than the whole." [1]

Financial institutions are adopting LSIS in order to meet competitive pressures, increase timeliness of information, foster operational efficiency, and ease introduction of new products. A commitment to LSIS sets the course of an institution's technology, management information system, and delivery systems for several years. Successful implementation of LSIS requires careful planning by both senior management and the board of directors.

[1] Christopher K. Heaney, "Who are these guys anyway?" ABA Banking Journal, May 1986, pp. 84-85 and development process. When these projects experienced lengthy delays, the financial institutions not only suffered large monetary losses but also delays in product development and a loss in their competitive positions.

Ineffective planning caused several financial institutions and software companies to spend millions of dollars and years of conversion and implementation time on LSIS, only to implement a portion of the system or in some cases abandon the project altogether. In many instances, the software vendors depended upon substantial ongoing investment by the financial institutions to fund the vendor's research

Concerns

Financial institutions have underestimated the cost, time and personnel resources required for the successful installation of LSIS. Therefore, time and cost targets should be established at the beginning of the project and closely reviewed by senior management on an ongoing basis.

In certain cases LSIS projects were abandoned because of the financial instability of software vendors. To prevent these situations from recurring, the financial condition and viability of each prospective vendor must be considered when evaluating systems.

Data backup and recovery measures for integrated systems are often more costly than those required for single application systems. In certain situations, the data base may require simultaneous backup. The additional costs for backup and recovery must be evaluated when determining the feasibility of LSIS.

If the system provides for instantaneous update of information – in other words, the user has direct access to the data – existing security systems may not be adequate. Thus, data security features must be evaluated to ensure that sufficient controls exist for LSIS.

Seemingly simple program changes can have unpredictable results in a mixed-application system. Thus, system development life cycle methodologies, which identify the sequence of activities required in the systems development process and throughout the useful life of the software, may need to be modified.

There is an increased possibility of unwarranted data manipulation and at the same time, there is less of an audit trail in an LSIS environment. Therefore, EDP audit coverage should be reviewed at the onset to determine whether specialized audit techniques are needed.

Board of Directors and Senior Management Responsibilities

The decision to acquire or develop in-house large-scale integrated software should be preceded by a strong and independent management planning process. This should include a thorough examination of existing software performance. Also, a detailed analysis of the system's capability to meet the institution's strategic business plans is essential.

The complexity of the software and its impact on the entire organization require a commitment from top management for the project to be successful. Responsibility for the conversion should be clearly identified and established at the senior management level.

Senior management should regularly review the project's status. This improves control over the complex process of implementation and ensures completion within established time and cost targets. It is particularly important that the board continue its oversight responsibilities after implementation.

The attached pages discuss the impact and responsibilities associated with LSIS.

SP-4 - APPENDIX
Large-scale Integrated Financial Software Systems

Definition and Scope

Large-Scale Integrated Systems (LSIS) are sophisticated software products which provide interconnections and facilitate the exchange of information between applications and functions. The integration architecture may be horizontal, tying together applications, such as deposits, loans, and general ledger. Alternatively, the architecture may be vertical, tying together functions, as in teller transactions being linked immediately to all operating departments. These systems are designed so that each application no longer exists individually but operates as part of a unified system. They often employ data base management technology, which increases the complexity of the system. LSIS processing may employ combinations of batch, online, or memo methods. A variety of LSIS are being marketed and others are in various stages of development.

Small-to-medium size financial software systems whose applications simply interfaced through a Central or Customer Information File (CIF) have been operating for many years. Many of these systems have been successfully installed and have operated properly for a considerable period. These systems are not included in the scope of this issue paper, although they are sometimes described as "integrated systems.

Advantages of Large-Scale Integrated Systems

- Provide tools to increase product line and customer relationships, ultimately increasing fee income on deposit and loan services.
- Enable financial institutions to meet competition generated from forces outside the banking industry.
- Lower the unit processing costs through standardization of operating techniques.
- Eliminate redundancy in data files.
- Provide information at more points throughout the institution, enabling faster and more accurate management decisions.

Disadvantages of LSIS

- The complexity and size of large-scale integrated systems can lead to underestimation of the time and resources needed for successful installation of these systems.
- The magnitude of the installation effort requires more comprehensive management techniques and project control.
- The financial instability of the software vendor may require the institution to furnish unplanned additional financial support to maintain contemplated service levels.
- The failure to properly install the software can lead to significant losses to the institution, in terms of time and resources expended, and a decline in competitive position.

Internal Control Related Concerns

- Data Security: Data security should be addressed prior to the installation of such a system. Existing data security systems may not be adequate for a complex integrated

system, particularly one using on-line real-time processing. Each individual function should be controlled, e.g. access controls, file maintenance, inquiry, and new accounts.

- EDP Auditing: A greater chance of unwarranted data manipulation and a diminished audit trail exists. Therefore, institutions should recognize the need for expanded EDP audits of this technology, especially in an on-line real-time environment.

  - Absence of Acceptable Audit Trails – When a system allows the automatic generation of a transaction prompted by a prior transaction, controls must be designed within the system to ensure satisfactory audit trails. This is especially critical considering that a single transaction may generate several other transactions.

  - Accountability for all transactions must be maintained through audit trails. Otherwise, system integrity deficiencies will jeopardize the software system's ability to provide a consistent product, as well as compromise internal controls.

  - Absence of Comprehensive Audit Software – Existing generalized audit software may not be readily adaptable for use with large-scale integrated systems, and may not be sufficiently sophisticated to follow an audit trail of all transactions generated by the system. Provision for audit software should be made at the time of system acquisition.

- Disaster Recovery Planning: Integrated systems have unique features which will require a thorough consideration of contingency requirements in the initial feasibility study. The complexity of the integration, horizontally, vertically, or both, may determine that current industry standards for the backup of hardware, software, data and communications are no longer applicable. A determination should be made how the institution, as a whole, will recover and how recovery will be addressed along functional lines. Subsequently, required testing may pose cost, logistical or other problems which will have to be resolved to ensure a viable disaster recovery plan.

- Changes in System Development Life Cycle (SDLC) Methodology: There are several significant control issues regarding the use of traditional SDLC methods with large-scale integrated systems. Current system development techniques may not permit the timely development and implementation of a complex system. SDLC techniques may need to be revamped to provide for increased flexibility. However, control and management methods may vary according to the complexity of the system under development.

  Minimum SDLC standards should ensure that project development is sufficiently controlled to provide for the integrity of the system. Testing of various stages within large scale integrated systems may require innovative techniques.

  Management should carefully consider the cost of the extensive user involvement in the system development stage. User involvement is necessary to ensure the successful implementation of a large scale integrated system.

  Management must provide more comprehensive employee training since the adoption of a LSIS will affect all departments.

  SDLC standards need to be flexible, while still providing for the maintenance of system integrity during development to ensure that a system of internal control is maintained.

Federal Financial Institutions Examination Council

SP-5
July 1989

Subject: Interagency Policy On Contingency Planning For Financial Institutions

To: Chief Executive Officers of all Federally Supervised Financial Institutions, Senior Management of each FFIEC Agency, and all Examining Personnel

Purpose

The purpose of this policy statement is to alert the Board of Directors and management of each financial institution to the need for contingency planning for their institution. This includes both institutions that provide their own information processing service and those that receive processing from service companies. The policy statement also addresses issues that should be considered when developing a viable contingency plan.

Background

Contingency planning is the process of identifying risks from disruption of operations and services. The objectives are to:

- minimize disruptions of service to the institution and its customers,
- minimize financial loss, and,
- ensure a timely resumption of operations in the event of a disaster.

These strategies are the same for institutions with in-house data centers and those using service bureaus.

In recent years, information technology has expanded rapidly throughout the corporate structure of financial institutions. It includes operations such as central computer processing, distributed processing, end user computing, local area networking, and nationwide telecommunications. These operations often represent critical services to institutions and their customers. The loss or extended disruption of these business operations poses substantial risk of financial loss and could lead to the failure of an institution. As a result, contingency planning now requires an institution-wide emphasis, as opposed merely focusing on centralized computer operations.

Additionally, there are many service bureaus that provide information processing services to multiple financial institutions. The disruption of the processing capabilities of one of these service bureaus could impact a considerable number of institutions. Accordingly, contingency planning by financial institution servicers is equally important.

Concerns

Many financial institutions and servicer bureaus have not sufficiently addressed the risks associated with the loss or extended disruption of business operations. More specifically:

- Many contingency plans do not address all of the critical functions throughout the institution.
- Many serviced institutions have not established or coordinated contingency planning efforts with their service bureaus.
- Many service bureaus have not established contingency plans.
- Many contingency plans have not been adequately tested.

Policy

The board of directors and senior management of financial institutions are responsible for:

- Establishing policies, procedures and responsibilities for comprehensive contingency planning
- Reviewing and approving the institution's contingency plans annually, documenting such reviews in board minutes.

If the institution receives information processing from a service bureau, management also must:

- Evaluate the adequacy of contingency plans for its service bureau.
- Ensure that the institutions contingency plan is compatible with its service bureau's.

The appendix to this policy statement provides an example of a process that management may consider in developing contingency plans. It is a brief outline and is not all encompassing. Each financial institution needs to assess its own risks and develop strategies accordingly. This planning process needs to address each critical system and operation, whether performed on site, at a user location, or by another company.

SP-5 - APPENDIX
Contingency Planning Process

I. Obtain commitment from senior management to develop the plan.

II. Establish a management group to oversee development and implementation of the plan.

III. Perform a risk assessment.

Consider possible threats such as:

- natural – fires, flood, earthquakes, ...
- technical – hardware/software failure, power disruption, communications interference, ...
- human – riots, strikes, disgruntled employee, ...

Assess impacts from loss of information and services:

- financial condition
- competitive position,
- customer confidence
- legal/regulatory requirements.

Analyze costs to minimize exposures.

IV. Evaluate critical needs.

- functional operations
- key personnel
- information
- processing systems
- documentation
- vital records
- policies/procedures

V. Establish priorities for recovery based on critical needs.

VI. Determine strategies to recover.

- facilities
- hardware
- software
- communications
- data files
- customer services
- user operations
- MIS
- end-user systems
- other processing operations.

VII. Obtain written backup agreements/contracts.

- facilities
- hardware
- software
- vendors

- suppliers
- disaster recovery services
- reciprocal agreements

VIII. Organize and document a written plan.

Assign responsibilities.

- management
- personnel
- teams
- vendors

Document strategies and procedures to recover.

- procedures to execute the plan
- priorities for critical vs. non-critical functions
- site relocation (short-term)
- site restoration (long-term)
- required resources
  - human
  - financial
  - technical (hardware/software)
  - data
  - facilities
  - administrative
  - vendor support

IX. Establish criteria for testing and maintenance of plans.

Determine conditions and frequency for testing.

- batch systems
- on-line systems
- communications networks
- user operations
- end-user systems

Evaluate results of tests.
Establish procedures to revise and maintain the plan.
Provide training for personnel involved in the plan's execution.

X. Present the contingency plan to senior management and the Board for review and approval.

(Note: Additional guidelines in this area are available in Chapter 10 of the 1996 FFIEC IS Examination Handbook). Also, many materials on contingency/disaster recovery planning have been published by trade associations, accounting firms, and the disaster recovery industry. These can be valuable guides to comprehensive contingency planning.

Federal Financial Institutions Examination Council

SP-6
January 1990

Subject: Interagency Statement on EDP Service Contracts

To: Chief Executive Officers of all Federally Supervised Financial Institutions, Senior Management of each FFIEC Agency, and all Examining Personnel

Purpose

This interagency statement alerts financial institutions to potential risks in contracting for EDP services and/or failing to properly account for certain contract provisions.

Issue

Some financial institutions are entering into EDP servicing contracts that contain provisions which may adversely affect the institution. Contract provisions may include extended terms (up to ten years), significant increases in costs after the first few years, and/or substantial cancellation penalties.

In addition, some service contracts improperly offer inducements that allow an institution to retain or increase capital by deferring losses on the disposition of assets or avoiding expense recognition for current charges. Institutions experiencing earnings and capital problems are particularly attracted to these inducements.

Examples of inducements include:

- The servicer purchasing assets (e.g., computer equipment or foreclosed real estate) at book value, which exceeds current market value;
- The servicer providing capital by purchasing stock from the institution;
- The servicer providing cash bonuses to the institution once the conversion process is complete; and
- The institution deferring expenses for conversion costs or processing fees under the terms of a lease or licensing contract.

These inducements offer a short-term benefit to the institution. However, the servicer usually recoups its costs by charging a premium for the data processing services it provides. These

excessive data processing fees adversely affect an institution's financial condition over the long-term. Furthermore, the institution's accounting for such inducements typically is inconsistent with generally accepted accounting principles (GAAP) and regulatory reporting requirements.

Title II, Section 225 of the Financial Institutions Reform, Recovery and Enforcement Act of 1989 states:

> An (FDIC) insured depository institution may not enter into a written or oral contract with any person to provide goods, products or services to or for the benefit of such depository institution if the performance of such contract would adversely affect the safety or soundness of the institution.

Accordingly, when negotiating contracts, an institution must ensure that the servicer can provide a level of service that meets the needs of the institution over the life of the contract. It is also the responsibility of the institution to ensure that contracts are accounted for in accordance with GAAP.

In summary, contracting for excessive servicing fees and/or failing to properly account for such transactions is considered an unsafe and unsound practice. Servicing agreements that include contract provisions or inducements similar to those discussed above should be closely reviewed by the institution. Institutions must ensure that accounting under such agreements reflects the "substance" of the transaction, not merely the "form."

Although this statement focuses on contracting for EDP services, these same issues may exist in contracts for other vital services.

Federal Financial Institutions Examination Council

SP-7
March 1990

Subject: Interagency Policy on Strategic Information Systems Planning for Financial Institutions

Purpose

This policy issuance alerts all financial institutions to the importance of strategic information systems planning and its role in overall corporate management and planning. It identifies management's responsibilities in preparing strategic plans for their information systems requirements.

Background

Information is a valuable corporate asset which is vital to the success of all financial institutions. The ability to remain competitive, introduce new products and services, and attain desired corporate goals often depends on the effective management of information systems technology.

Corporate level strategic planning is important in all financial institutions to effectively utilize available resources and achieve the long term goals and objectives of the organization. Strategic information systems planning is integral to the overall corporate strategic planning process and must support individual business strategies throughout the institution. The information systems strategic plan should address technology risks affecting all areas of operation, including contingency planning and disaster recovery, information security, systems and programming, computer operations, and end-user computing.

Effective strategic planning considers the impact of technology on the internal and external concerns of the institution. Internal issues are those where management has planning control. This includes profitability, delivery of new products and services, efficient and consistent operations, and corporate strategic planning. External issues are those over which management has no direct control, but must react to in a timely manner. These include technological advancements by competitors, regulatory requirements, and changing economic environments.

Strategic information systems planning is generally structured to address two primary objectives.

1. Build a technology strategy to assure that systems are:

- Cost effective in meeting business objectives;
- Timely (i.e. available when needed);
- Flexible (i.e. expandable/contractible);
- Efficient (i.e. competitive parity and competitive advantage); and

- Reliable (i.e. complete and accurate data).

2. Provide a system architecture integrating hardware, software, and telecommunications to assure:

   - Proper collection and processing of information;
   - Availability of information, as required, at different locations; and
   - Proper distribution of applications.

Policy

Financial institutions should develop and implement a written strategic information systems plan commensurate with the complexity and sophistication of the institution. The plan should be integrated into overall corporate goals and should include in-house, end-user, and service bureau processing, as applicable. Successful implementation of a strategic information systems plan requires the board of directors of an institution to:

- Provide adequate oversight, including the review and approval, of business objectives and related information systems strategies;

- Ensure the ongoing development and implementation of the information systems plan;

- Ensure the technology strategy considers the size and complexity of the institution, the markets it pursues, and the nature of the products and services it offers; and

- Ensure the design of the organizational structure includes well defined delegations of authority commensurate with information systems technology.

The attached appendix provides additional guidance relating to strategic information systems planning.

SP-7 - APPENDIX
Board of Directors Oversight

The board of directors is responsible for reviewing and approving corporate strategies to ensure the continuance of successful operations. Oversight includes periodic review and approval of overall business objectives. This review should ensure coordination of the information systems plan with the overall corporate strategic plan. The monitoring process should reflect changes in current systems development. These changes should be reported in summary format in board and steering committee minutes.

Oversight activities include:

- Reviewing cost benefit analyses;
- Monitoring periodic performance/status reports;
- Ensuring that goals are consistent with overall corporate goals and safety and soundness;
- Implementing the plan through the effective utilization of financial resources, personnel skills and methodologies;
- Reviewing contingency/recovery policies on an annual basis; and
- Evaluating acquisition/merger conversion plans.

The following diagram and definitions illustrate the flow and structure of the planning hierarchy:

Corporate Strategic Goals	→	Board of Directors
Strategic Plan	→	Senior Management
	→	Middle Management
Tactical Plan	→	Steering Committee
Operational Plan	→	Operational Groups

CORPORATE STRATEGIC GOALS

The board of directors establishes long term corporate goals and objectives for the financial institution. More specifically, the board determines the institution's current market position, methods needed to gain a competitive edge, and resources required to achieve the desired goals.

STRATEGIC PLAN

This plan defines the future direction and mission of the institution. It may be revised every two years and encompasses a time span of three to seven years. Its scope includes target markets, resources, technologies, and other appropriate criteria. Results show a framework and vision for

the institution's future direction. This plan is the backbone for supporting tactical plans.

TACTICAL PLAN

This is a program of action over a two-to five-year time period. It is updated annually and focuses more narrowly on the broad scope identified in the strategic plan. It results in a determination of specific activities, budgets, opportunities, and functional objectives.

OPERATIONAL PLANS

Often these plans list specific actions and milestones by month to achieve project plans, budgets, management by objective (MBO) agreements, and commitments. The plan life-cycle is generally for one year and can be subject to numerous updates and revisions.

Federal Financial Institutions Examination Council

SP-8
September 1991

Subject: Interagency Document on EDP Risks in Mergers & Acquisitions

To: Senior Management of each FFIEC Agency

Background

In recent years, mergers and acquisitions within the financial industry have increased significantly. With the changes in interstate banking laws many financial institutions have pursued mergers and acquisitions to enhance asset growth, gain market penetration, and to achieve a competitive advantage over rival institutions.

During the week of May 7, 1990 senior EDP examiners of the FFIEC member agencies participated in an EDP Symposium to examine the risks associated with mergers and acquisitions. To gain as broad a perspective as possible, various authorities, including agency regulators involved in the applications process, senior management responsible for information system conversions and consultants were invited to share their experience on the subject. The symposium participants addressed areas of concern, identified risks associated with mergers and acquisitions, and prepared conclusions and recommendations.

Findings

Historically, financial institutions have acquired significantly smaller institutions and have integrated the acquired institution into an existing organizational structure. In the past several years financial institution regulators have seen the consummation of mergers and acquisitions which have necessitated the development of new and complex information systems. One result is the consolidation of data processing systems and back office operations.

While a merger or acquisition may require the financial institution to engage in a system conversion, it should be noted that many conversions are unrelated to mergers or acquisitions. While there are risks associated with any conversion, well managed strong institutions have generally been able to overcome conversion problems successfully while weaker institutions have been adversely affected. Financial institutions have encountered unanticipated problems in the conversion process that have had implications throughout the institution. These include:

- An adverse impact on profitability;
- The reporting of inaccurate financial information to regulatory agencies;

- The inability to reconcile general ledger accounts;
- Management decisions based on inaccurate information; and
- A negative impact on public confidence.

Documented cases involving conversion-related data processing problems which examiners have reported include the following:

- A large money center bank was unable to complete processing for 32,000 trades of government securities, resulting in an overdraft of $32 billion at the Federal Reserve;
- A large holding company experienced a $4 billion out-of-balance condition following a change in its check processing system;
- As the result of a faulty general ledger system conversion, a thrift institution chronically filed late and inaccurate regulatory reports, resulting in civil money penalties being assessed; and
- As the result of a faulty check processing system conversion, a thrift institution was forced to charge off unresolved bookkeeping differences equivalent to one year's net income.

Poorly planned mergers have also resulted in systems conversions that have extended beyond projected time frames, resulting in unanticipated expenses and/or unrealized cost savings. Traditionally, mergers and acquisitions were accomplished within the confines of existing systems and, with adequate pre-planning, were effected in a short period of time. In the current merger and acquisition environment, where mergers of equal size institutions are not uncommon, the potential for an unsuccessful conversion is greatly increased. A 1989 survey by Ernst & Young and Keefe, Bruyette & Woods, Inc. of 34 banks and bank holding companies with assets over $6 billion which were involved in mergers and acquisitions showed that in mergers of equals, neither bank had the capacity to absorb the data processing and back office operations of the other. Additionally, in this type of transaction, institutions have been able to reduce data processing and operations expense by amounts substantially below projections. The survey also showed that most of the institutions had extensive experience with acquiring smaller financial institutions while only a few had been involved in a merger with another large financial institution.

Conclusions

Symposium participants concluded that the following factors increase the potential for an unsuccessful or problem conversion:

- Insufficiently detailed plans;
- Failure to commit necessary resources;
- Failure to retain personnel necessary to effect a successful conversion;
- Inadequate controls which result in reconcilement and system problems; and
- Inaccurate reports produced by information systems.

RECOMMENDATIONS

To minimize the risks associated with mergers and acquisition involving conversions of information systems, regulators should:

- Determine the impact of these activities on EDP and other examination strategies. Examples of significant EDP conversions include: major application changes, initial conversion to in-house operations, outsourcing major applications, operating systems enhancements, and data security revisions;

- Review the institution's EDP plans for effecting the merger or acquisition as part of the application process; and

- Monitor the status of merger and acquisition activities involving data centers under their supervisory authority.

Federal Financial Institutions Examination Council

SP-9
April 1993

Subject: Interagency Supervisory Statement on EFT Switches and Network Services

To: Chief Executive Officers of all Federally Supervised Financial Institutions, Senior Management of each FFIEC Agency, and all Examining Personnel

Purpose

The purpose of this supervisory issuance is to alert the Board of Directors and senior management of financial institutions to the risks associated with switch and network services in retail electronic funds transfer (EFT) systems. This statement does not address wholesale or large dollar funds transfer systems such as FEDWIRE and CHIPS.

Definitions

A switch is a computer system that facilitates the transfer of electronic messages between terminal devices and the appropriate network participants. For example, it transmits an inquiry or transaction from an automated teller machine (ATM) or point-of-sale (POS) terminal to the depository institution that holds the customer's account. EFT terminals, processors, and switches can be configured in many different ways, depending on the participants' needs. The combination of interconnected terminals and computers is a network. Networks are sometimes operated by independent third party servicers.

Background

Financial institutions have increased the use of switch and network services to lower costs and improve competitive position. Many financial institutions are sharing resources or using outside servicers, including non-financial companies, to provide EFT services. Such services include POS, ATM, and bill payment. Industry marketing efforts are promoting additional shared retail services, such as automated clearing houses (ACH), stored value cards, and credit card authorization.

EFT switches and network processing systems have expanded traditional methods of consumer banking, e.g., deposit, withdrawal, and obtaining credit. These systems provide customers with regional or nationwide access to their funds.

Some financial institutions are required by state law to share these services. Others voluntarily share them on a regional, national, or international basis.

Examples of shared EFT switch and network services include:

- A multi-bank holding company network servicing affiliated institutions;
- A network formed and shared by different types of financial institutions; and
- A non-financial company's proprietary network shared with financial institutions for a fee.

Regardless of the types of services offered or systems being used, there are inherent risks in switch and network services.

Concerns

The increasing use of switches and networks raises certain concerns for participants:

- OPERATIONAL FAILURE: System failure or service interruption, which may be caused by a disaster, could impact all connected financial institutions and could cause an erosion of consumer confidence;
- SETTLEMENT FAILURE: Network participants could fail to make required settlement payment, resulting in significant financial losses; or, the processor could fail to provide necessary settlement records, forcing participants to reconstruct transactions;
- FINANCIAL FAILURE: The switch servicer could experience sudden financial problems that may adversely impact all connected financial institutions;
- DOLLAR LIMITS: The network's dollar limits, such as those applied to withdrawals, may be different from the limits the institution established;
- AUDIT COVERAGE: Audits may not sufficiently cover internal controls, enforcement of standards, and review of transactions processed;
- CONTRACTS: Poorly written contracts may inadequately define participants' liabilities and responsibilities and expose financial institutions to potential loss.

Summary

The Board of Directors and senior management of financial institutions are responsible for:

- Ensuring that controls covering the switch processing environment are adequate. Alternatives to accomplish this objective include qualified internal or external auditors, or consultants specializing in this area. The results of these evaluations, and management's efforts toward correction, need to be documented in Board minutes.
- Ensuring that contracts for switches and network services are reviewed by legal counsel and meet minimum regulatory contract servicing guidelines. The guidelines are detailed in the FFIEC Interagency Statement on EDP Service Contracts (SP-6) and the FFIEC EDP Examination Handbook.
- Ensuring that settlement procedures do not pose undue risk to their institutions and that network rules adequately address actions that would be taken in the

event that a participating institution fails to settle.

The appendix to this statement provides controls that should be in place in an EFT switch or network services environment.

SP-9 - APPENDIX
Control Objectives

Control for a safe and sound EFT network switching environment should address the following items. These objectives apply to all EFT switches and network servicers regardless of ownership:

Management:

- Written, approved, and enforced policies and procedures covering personnel, security controls, operations, and disaster recovery;
- Adequate segregation of duties and responsibilities;
- Periodic control evaluations of the switch and network;
- Daily settlement of switch activity and balancing of network activity, and periodic verification of fee distribution;
- Contracts that identify the responsibility and liability of all parties (e.g., timely presentment of returned items and appropriateness of fees and surcharges); and
- Adequate fidelity and business interruption insurance.

Security:

- Physical access restrictions;
- Encryption of critical data elements (e.g., personal identification code);
- Adequate management of encryption keys used in software;
- Software access controls including the program library, data files, and the network;
- Controlled access to positive and negative card files, used to authorize transactions; and institution control files (ICF) or institution parameter blocks (IPB), used to store institution-specific processing criteria; and
- Captured card procedures.

Operations:

- File backup and disaster planning including telecommunications;
- Audit trails sufficient to trace transactions through the system;
- Stand-in processing (having the cardholder data available at the switch for authorization) procedures should be available in the event of processor downtime, including the handling of positive balance files (PBF) and cardholder authorization systems (CAS);
- Restart and recovery procedures to ensure the continuity of transaction processing in the appropriate sequence;
- Controls over the embossing, encoding and distribution of access devices; and
- Controls over the generation of cardholder personal identification codes (PIC) and communication of PICs to cardholders.

Federal Financial Institutions Examination Council

SP-10
December 1993

Subject: Control And Security Risks in Electronic Imaging Systems

To: Senior Management of Each FFIEC Agency and All Examining Personnel

Purpose

This issuance advises the senior management and examining personnel of each FFIEC agency of risks associated with electronic imaging systems in financial institutions.

Definition

Electronic imaging systems is a term that describes the technology used to capture, index, store and retrieve electronic images of paper documents.

Background

Technological advances in document scanning and optical character recognition are replacing the traditional paper storage systems in financial institutions. These systems incorporate new technologies such as optical disk storage, high resolution displays, document scanners, and laser printers to capture, store and print documents. Once stored in electronic form, the documents can be accessed throughout the organization. Image systems can range from small systems supporting a business function or department with a few users, to large systems or networks supporting multiple departments with hundreds of users.

Imaging systems replace the handling, distribution and storage of paper documents with electronic images. They are generally grouped into two types of systems: Document Management Systems and Item Processing Systems.

Document Management Systems

Document management imaging systems automate the flow of paper documents processed by departments and offices in a financial institution. These applications are referred to as "lowspeed" imaging systems as documents contained in office or customer file folders are scanned one at a time. The process consists of capturing original documents in electronic form on a lowspeed scanning device, entering additional data and text into the record via keyboard entry, indexing the file folder and documents in a computer data base, and storing the folder on electronic storage media. Documents can then be displayed on a computer terminal, processed, or printed at work stations throughout the organization. These systems allow for the automatic routing of electronic documents to those individuals involved in the review or decision making process. They can also

route documents or file folders for quality control reviews.

Document management systems account for the majority of imaging systems in financial institutions today. Examples of business functions where original documents (loan applications, customer correspondence, etc.) are being converted to imaging systems to improve processing and customer service are:

- customer service account inquiries
- student loan processing
- loan/mortgage servicing applications
- IRA/Keogh files
- trust files
- signature verifications
- accounts payable

Item Processing Systems

Item processing imaging systems automate check or remittance processing applications on reader-sorters or similar high speed capture equipment. Images of transaction items are captured and stored for later use in encoding documents and exception processing. Item processing imaging systems require special attention to the quality and readability of the imaged documents. These high speed systems are relatively expensive to install as they require special scanning equipment, expanded storage capacity, and complex software programs to convert documents into readable electronic images.

Examples of item processing applications where transaction documents are converted to images for processing are:

- proof-of-deposit
- sales draft (credit card/POS) processing
- remittance processing
- account reconciliation processing
- statement rendering

Control and Security Risk Areas

The replacement of paper documents with electronic images can have a significant impact on the way that an institution does business. Many of the traditional audit and security controls for paper based systems may be reduced or absent in electronic document workflow. New controls must be developed and designed into the automated process to ensure that information in image files cannot be altered, erased or lost.

Risk areas that management should address when installing imaging systems, and that examiners should be aware of when examining an institution's controls over imaging systems, are listed below:

Planning – The lack of careful planning in selecting and converting paper systems to document imaging systems can result in excessive installation costs, the destruction of original documents, and the failure to achieve expected benefits. Critical issues such as converting existing paper storage files, integration of the imaging system into the organization workflow, and equipment backup and recovery procedures should be addressed to avoid reduced customer service and business interruptions.

Audit – Imaging systems may change or eliminate the traditional controls, and checks and balances inherent in paper based systems. Audit procedures may have to be redesigned, and new controls designed into the automated process. Audit departments should be sufficiently involved to ensure that electronic document workflows include appropriate audit controls and audit trails.

Redesign of Workflow – Institutions generally redesign or reengineer workflow processes to benefit from imaging technology. New jobs or functions are identified and others eliminated. Changes may range from the redesign of forms to the reorganization of departments. Traditional controls such as time/date stamps, control numbers, review signatures, etc. may be replaced by limiting access to imaged documents, automated logs that report document access and retrieval information, etc. The absence of these, and other automated controls, may result in increased risks for the institution.

Scanning Devices – Scanning devices are the entry point for image documents and a significant risk area in imaging systems. Scanning operations can disrupt workflow if the scanning equipment is not adequate to handle the volume of documents, or the equipment breaks down. The absence of controls over the scanning process can result in poor quality images, improper indexing, and incomplete or forged documents being entered into the system. Factors that should be considered in an imaging system are quality control over the scanning and indexing process, the scanning rate of the equipment, the storage of images, equipment backup, and the experience level of personnel performing the scanning function.

Indexing – Poorly designed imaging system indexes can result in lost or inaccessible documents. Proper indexing of scanned documents is critical to later retrieval, and establishing access levels to individual documents and file folders. The integrity of indexes must be carefully maintained to ensure access to all documents and protection from unauthorized modification. The indexing method can affect the security administrator's ability to restrict access to documents or file folders. The institution should maintain automated journals and audit trails of document access and modifications to customer records.

Software Security – Security controls over image system documents are critical to protect institution and customer information from unauthorized access and modifications. The integrity and reliability of the imaging system database is directly related to the quality of the controls over access to the system. Software security and security administrator functions are essential to prevent unauthorized alterations to stored documents.

Contingency Planning and Backup Procedures – Since more than 100,000 documents may be stored on a single optical disk, the loss of electronic image files or storage media can severely impact business operations if back-up electronic or paper files are not readily available. Contingency planning and back-up storage procedures for imaging system documents should follow generally accepted practices for data processing and management information systems.

Training – Inadequate training of personnel scanning documents can result in poor quality document images and indexes, and the early destruction of original documents. The installation and use of imaging systems can be a major change for department personnel. They must be adequately trained to ensure quality control over the scanning and storage of imaged documents, as well as the use of the system to maximize the benefits of converting to imaging systems.

Legal Issues – Case law on the admissibility of electronic image as evidence has not yet been established by the courts. Although precedent has been established on related electronic documents such as facsimile, microfilm, and photocopies, the courts have not addressed the authenticity of electronic images of original documents. Institutions installing imaging systems

should carefully evaluate the legal implications of converting original documents to image, and the subsequent destruction of the original documents.

Conclusion

Imaging systems offer institutions benefits in streamlining department and office workflow processes, reduced storage and retrieval costs, and improved customer service by automating customer files and
correspondence. These systems present new concerns and challenges for examiners and board of directors who must ensure that the risks are addressed by the institution's management.

Federal Financial Institutions Examination Council

SP-11
January 1995

Subject: Enhanced Supervision Program for Multidistrict Data Processing Servicers (MDPS)

To: Senior Management of Each FFIEC Agency and All IS Examining Personnel

Objective

To establish guidelines to improve the supervision of and communication with the independent data processing service vendors in the Multidistrict Data Processing Servicers program.

Background

The MDPS examination program presently covers 17 nonbank EDP vendors that provide key data processing services to more than half of the federally insured depository institutions. In recent years, many of the country's larger depository organizations have outsourced their EDP operations which has increased further the industry's dependence on outside service bureaus. Most vendors service institutions through regional data centers. The institutions depend on the quality and continuity of these services to conduct their business. Disruptions in services at a single vendor, as a result of either financial or operational conditions, could cause substantial systemic risk in the industry.

The core element of the interagency MDPS program continues to be the on-site Information Systems examination. The FFIEC's Interagency EDP Examination, Scheduling and Distribution Policy, as amended in 1991, identifies the frequency for examinations under the MDPS program. Those vendors, rated 1 or 2 are examined on a 24 month examination cycle; vendors rated 3, on an 18 month cycle; and vendors rated 4 or 5, on a 12 month cycle. As part of each examination, the agency-in-charge is responsible for formulating and implementing a supervisory strategy.

Enhanced Supervisory Program (ESP)

The ESP supplements existing on-site examinations with interim reviews of material changes in the vendor's activities and condition. The ESP should allow each agency to more promptly recognize and supervise risks associated with the concentration of services in vendors.

The interim reviews will follow up on matters from the previous examination, assess major changes (e.g. in the vendor's business plan, the number and type of financial institutions serviced, corporate/management structure, financial condition, and hardware and software), and plan subsequent reviews and examinations. The scope and frequency of the interim reviews will vary depending on the condition and/or degree of change in the vendor. However, vendors that are on a 24 month examination cycle are expected to receive a minimum of two interim reviews and vendors on 12 or 18 month cycles are expected to receive at least one interim review.

Reviews may be conducted through correspondence, telephone interviews, and/or other requests

for information if the agency-in-charge is able to obtain the information necessary to evaluate the vendor's condition and stay abreast of material changes in its activities and operations without going on-site to collect the information. Interim reviews for vendors rated 3, 4, or 5, and those experiencing major changes in their activities and operations, are expected to be on-site visits.

If visits are necessary they will be conducted at the corporate headquarters of the vendor and ordinarily will not include branch or subsidiary data center sites. However, if necessary, examiners may visit additional sites. If the agency-in-charge requires assistance from examiners from other agencies, the Subcommittee should be informed as early as possible to facilitate coordination.

Reporting

The agency-in-charge (AIC) will be responsible for preparing a brief summary memorandum documenting findings, conclusions, and recommendations from each interim review. That memorandum is an internal document and is not intended for distribution. The memorandum will be provided to the Subcommittee and shared with the agencies, as appropriate. The memorandum should include a brief discussion of:

(1) The vendor's progress in addressing recommendations presented in the last examination;

(2) The vendor's progress in addressing recommendations presented in selected internal and external audit reports;

(3) Any deterioration in financial condition or other matters that threaten the vendor's viability or its ability to continue to provide uninterrupted service;

(4) Recommendations regarding frequency, timing, scope, and locations of future reviews and examinations; and

(5) A listing of participating examiners, agencies and duration of participation.

At the conclusion of the interim review, a brief overview of the examiner's conclusions and any material findings or recommendations should be discussed with the vendor. Unless the agency-in-charge considers it necessary, there is no need for a formal close-out meeting with the vendor's directors or their designated compliance or audit committees.

If the agency-in-charge prepares separate written correspondence for the vendor, a copy of the letter will be provided to the Subcommittee.

Role of the Information Systems Subcommittee

In order for the Subcommittee to provide for consistency in the conduct of the program and to assure effective coordination and scheduling of examiner resources, the AIC will provide the Subcommittee with a strategy for supervising the vendors. That strategy will include information on the agency's proposed schedule and scope for the conduct of examinations and anticipated interim reviews. The Subcommittee will provide guidance to the member agencies in their conduct of interim reviews.

In developing this program, the Subcommittee has designed the frequency, scope, and reporting requirements for interim reviews so as not to require significant additional examiner resources for the supervision of vendors. The Subcommittee anticipates that the interim reviews will permit the AIC to be more familiar with the vendors and, therefore, will reduce the time spent on the examination.